REMARKS

In the non-final Office Action, the Examiner rejects claims 1-7, 9-11, and 22-25 under 35 U.S.C. § 103(a) as unpatentable over SYVANNE et al. (European Patent Application Publication No. 1,317,112) in view of KAVANAGH (U.S. Patent Application Publication No. 2003/0081607); and rejects claims 26 and 27 under 35 U.S.C. § 103(a) as unpatentable over SYVANNE et al. in view of KAVANAGH and GOPAL et al. ("User Plane Firewall for 3G Mobile Network"; Vehicular Technology Conference; IEEE 58th; Vol. 3, October 6, 2003). Applicants respectfully traverse these rejections.[1] Claims 1-7, 9-11, and 22-27 are pending.

Claims 1-7, 9-11, and 22-25 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over SYVANNE et al. in view of KAVANAGH. Applicants respectfully traverse this rejection.

Claim 1 recites a method of screening incoming packets that includes detecting a request to establish a connection from a first network to a packet data network; detecting establishment of a tunnel, wherein the tunnel has a support node at each end of the tunnel, one of the support nodes being a gateway to the packet data network, wherein the tunnel is used to convey user traffic and the user traffic through the tunnel can have one or more associated firewall sessions on a firewall outside the tunnel; inspecting packets in the tunnel to detect information associated with the firewall sessions; detecting a tear down of the tunnel in response to inspecting the packets; and sending a request to the firewall to clear the one or more firewall sessions in response to detecting the tear down of the tunnel. SYVANNE et al. and KAVANAGH, whether

[1] As Applicants' remarks with respect to the Examiner's rejections overcome the rejections, Applicants' silence as to certain assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, reasons for modifying a reference and/or combining references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or that such requirements have been met, and Applicants reserve the right to dispute these assertions/requirements in the future.

taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, SYVANNE et al. and KAVANAGH do not disclose or suggest detecting a tear down of a tunnel in response to inspecting packets in the tunnel to detect information associated with firewall sessions. The Examiner admits that SYVANNE et al. does not disclose this feature and relies on paragraphs 0010, 0013 and 0046-0047 of KAVANAGH as allegedly disclosing this feature (Office Action, pg. 4). Applicants respectfully disagree with the Examiner's interpretation of KAVANAGH.

At paragraph 0010, KAVANAGH discloses:

> FIG. 3 is a signaling diagram illustrating the GTP control messages utilized to delete a PDP Context and tear down a GTP Tunnel. The GTP Tunnel can be torn down by initiating a Detach Request 35, by either the operator or the MS 11. A mobile-originated detach request is sent to the SGSN 15 which, in turn, sends a Delete PDP Context Request message 36 to the GGSN 22. The GGSN deletes the PDP Context for this MS and responds with a Delete PDP Context Response message 37 to the SGSN. The SGSN sends an International Mobile Station Identifier (IMSI) Detach Indication 38 and GPRS Detach Indication 39 to the GGSN. The SGSN then deletes the PDP Context, and sends a Detach Accept message 40 to the MS. As a result, the GTP tunnel is deleted.

This section of KAVANAGH discloses the General Packet Radio Service Tunneling Protocol (GTP) control messages are used to tear down a GTP Tunnel. This section of KAVANAGH does not disclose or suggest inspecting packets to detect information associated with firewall sessions or detecting a tear down of the tunnel in response to inspecting the packets. In fact, KAVANAGH discloses that a GTP Tunnel is automatically torn down when transmission between two nodes connected by the GTP Tunnel is finished (paragraph 0007). Therefore, this section of KAVANAGH cannot disclose or suggest detecting a tear down of a tunnel in response to inspecting packets in the tunnel to detect information associated with firewall sessions, as recited in claim 1.

At paragraph 0013, KAVANAGH discloses:

> In one aspect, the present invention is directed to a method of filtering data packets in General Packet Radio Service (GPRS) Tunneling Protocol (GTP) signaling messages between service nodes in a GPRS network. The method includes the steps of analyzing at least one GTP signaling message against a plurality of filtering criteria, and responsive to the analyzing step, selectively dropping data packets from the GTP signaling message or allowing the packets to pass. The analyzing step may include analyzing messages selected from a group consisting of GTP Path Management messages, GTP Tunnel Management messages, GTP Mobility Management messages, and GTP Location Management messages. The analysis may include the steps of verifying that the data packets in the GTP signaling message contain correct source, destination, and mask addresses; verifying that the data packets in the GTP signaling message contain User Datagram Protocol/Transmission Control Protocol (UDP/TCP) port numbers that are consistent with the GTP version number; and inspecting the data packets at the GTP level, layer-5. Based on information in the GTP header and accompanying Information Elements (IEs), selected GTP packets are dropped.

This section of KAVANAGH discloses analyzing at least one GTP signaling message against a plurality of filtering criteria, and responsive to the analyzing step, selectively dropping data packets from the GTP signaling message or allowing the packets to pass. This section of KAVANAGH discloses inspecting packets, but does not disclose or suggest inspecting packets to detect information associated with firewall sessions or detecting a tear down of a tunnel in response to inspecting the packets. Therefore, this section of KAVANAGH cannot disclose or suggest detecting a tear down of a tunnel in response to inspecting packets in the tunnel to detect information associated with firewall sessions, as recited in claim 1.

At paragraphs 0046-0047, KAVANAGH discloses:

> Since no stateful inspection exists today to determine whether a particular message type is permitted, all GTP message types are passed through firewalls. GTP Packets are identified by firewalls today based on their port numbers and the source and destination IP addresses. As a result, today's firewalls are unable to control the rate at which GTP packets are sent and received to and from the GSN nodes in the PLMN network, and their neighboring PLMN networks with whom they have a roaming agreement. The firewalls are unable to prioritize message types for processing, and are unable to determine which message types are permitted to be passed to the GSN nodes to be further processed, or which messages should be dropped at the firewall. Thus, GTP can be used to launch DoS attacks against the GPRS PLMN operator's network and also for Tunnel Hijacking.
>
> FIG. 4 is a flow chart illustrating the overall method of filtering GTP packets in the preferred embodiment of the present invention. The source and destination IP addresses and port number are first checked before GTP filtering is started on the inbound/outbound packet. Based on information in the GTP header, accompanying

> Information Elements (IEs), and the GTP version number, GTP messages are filtered and selected GTP packets are blocked. At step 41, any or all of the Path Management messages utilized in the GTP protocol are analyzed. Based on the information in the GTP header, accompanying IEs, and the GTP version number, selected GTP packets are blocked. As shown at 42, the GTP Filter may select messages for analysis from a group that includes the GTP Echo Request and Echo Response messages.

This section of KAVANAGH discloses filtering GTP packets by blocking selected GTP packets based on information in the GTP header, accompanying Information Elements, and the GTP version number. This section of KAVANAGH discloses inspecting packets to determine if a packet should be blocked, not inspecting packets to detect information associated with firewall sessions. Furthermore, KAVANAGH does not disclose or remotely suggest detecting a tear down of a tunnel in response to inspecting the packets. Therefore, this section of KAVANAGH does not disclose or suggest detecting a tear down of a tunnel in response to inspecting packets in the tunnel to detect information associated with firewall sessions, as recited in claim 1.

In response to similar arguments made in the previous response, on page 2 of the Office Action, the Examiner states:

> Kavanagh teaches inspecting packets in the tunnel to detect firewall session information…by teaching a GTP tunnel…that has its messages pass through firewalls…The firewalls screen and filter the GTP tunnel packets and access information in the packets such as the header to determine whether the firewall session should reject the packet…Thus, Kavanagh teaches inspecting packets to detect information associated with the firewall session.

Applicants respectfully disagree. As noted above, KAVANAGH discloses that a GTP Tunnel is automatically torn down when transmission between two nodes connected by the GTP Tunnel is finished (paragraph 0007). KAVANAGH further discloses inspecting packets to determine if a packet should be blocked (paragraph 0047). KAVANAGH, however, does not disclose or suggest inspecting packets to detect information associated with firewall sessions or detecting a tear down of a tunnel in response to inspecting the packets. Therefore, KAVANAGH does not

disclose or suggest detecting a tear down of a tunnel in response to inspecting packets in the tunnel to detect information associated with firewall sessions, as recited in claim 1.

For at least the foregoing reasons, Applicants submit that claim 1 is patentable over SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination.

Claims 2-7 and 9-11 depend from claim 1. Therefore, these claims are patentable over SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, these claims recite additional features not disclosed or suggested by SYVANNE et al. and KAVANAGH.

For example, claim 2 recites detecting a tear down of a GTP tunnel within the first network. The Examiner relies on paragraph 0029 of SYVANNE et al. and paragraph 0010 of KAVANAGH as allegedly disclosing this feature (Office Action, pg. 4). Applicants respectfully disagree with the Examiner's interpretation of SYVANNE et al. and KAVANAGH.

To begin, the Examiner admits that SYVANNE et al. does not disclose detecting a tear down of a tunnel (Office Action, pg. 4). Therefore, SYVANNE et al. cannot disclose or suggest detecting a tear down of a GTP tunnel within the first network, as recited in claim 2.

Nevertheless, at paragraph 0029, SYVANNE et al. discloses:

> The data connectivity of the mobile entity may be through wireless or fixed line connection. Typically such mobile entities are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. The physical location independence of the mobile entities may be based on mobile IP, GTP or some other protocol. The system providing connectivity to the mobile entity may be but is not limited to LAN (Local Area Network), WLAN (Wireless LAN), GSM (Global System for Mobile communications), GPRS (General Packet Radio Service), or UMTS (Universal Mobile Telecommunications System).

This section of SYVANNE et al. discloses that the data connectivity of mobile entities may be through wireless or fixed line connections and the physical location of the mobile entities may be based on mobile IP, GTP, or some other protocol. While this section of SYVANNE et al.

mentions GTP, this section of SYVANNE et al. has nothing to do with detecting a tear down of a GTP tunnel within the first network, as recited in claim 2.

As noted above, at paragraph 0010, KAVANAGH discloses the General Packet Radio Service Tunneling Protocol (GTP) control messages used to tear down a GTP Tunnel. This section of KAVANAGH does not disclose or suggest detecting a tear down of a tunnel. Therefore, this section of KAVANAGH cannot disclose or suggest a tear down of a GTP tunnel within the first network, as recited in claim 2.

For at least these additional reasons, Applicants submit that claim 2 is patentable over SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination.

Independent claim 22 recites a system for screening incoming packets that includes a GTP firewall including a GTP communication module; and a Gi firewall that includes: a Gi communication module that is operable to receive an instruction from the GTP communication module to tear down a firewall session, a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module. SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, SYVANNE et al. and KAVANAGH do not disclose or suggest a Gi firewall that includes a Gi communication module that is operable to receive an instruction from a GTP communication module of a GTP firewall to tear down a firewall session, a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module. The Examiner appears to rely on paragraphs 0022 and 0041 of SYVANNE et al. and on paragraphs 0010 and 0046 of KAVANAGH as allegedly disclosing this feature (Office Action,

pg. 6). Applicants respectfully disagree with the Examiner's interpretation of SYVANNE et al. and KAVANAGH.

At paragraph 0022, SYVANNE et al. discloses:

> The firewall receives from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall. On the basis of the received mobile entity table the firewall updates (deletes, adds or modifies entries) its second mobile entity table and deletes an entry in its first mobile entity table, if a corresponding entry is contained in the received mobile entity table. Receiving an entry of the first mobile entity table in a mobile entity table of some of the firewall indicates that the corresponding entity has moved from the firewall to the other firewall and may therefore be deleted from the first mobile entity table of the firewall as unnecessary. The state information associated with the mobile entity are in practice queried from the firewall by the other firewall before deleting the corresponding entry in the first mobile entity table of the firewall. Alternatively, entries of a first mobile entity table may be removed also on the basis of a time.

This section of SYVANNE et al. discloses that a firewall updates a second mobile entity table by deleting, adding or modifying entries, and deletes an entry in a first mobile entity table if a corresponding entry is contained in the received mobile entity table. SYVANNE et al. discloses sharing information between firewalls that connect subnetworks to a public network (Fig. 2A, paragraph 0032). SYVANNE et al. further discloses that the firewall system that connects a subnetwork to a private network does not have information about the connections inside the subnetwork (paragraph 0032). Therefore, SYVANNE et al. cannot disclose or suggest a Gi firewall that includes a Gi communication module that is operable to receive an instruction from a GTP communication module of a GTP firewall to tear down a firewall session, a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module, as recited in claim 22.

At paragraph 0041, SYVANNE et al. discloses:

> A firewall according to the invention sends the first mobile entity table to a predefined set of other firewalls as a response to a predefined action. Figure 5 is a flow diagram illustrating exemplary methods for triggering sending a mobile entity table to other

> firewalls. In step 500 it is checked, if a predefined time period has elapsed since the first mobile entity table was sent the last time. If is has, the first mobile entity table is sent in step 502 to a predefined set of other firewalls. In step 504 it is checked, if the content of the first mobile entity table has changed. If is has, the first mobile entity table is sent in step 502 to a predefined set of other firewalls. This may be done also so that when ever an entry is added, deleted or modified in the first mobile entity table, it is sent to the other firewalls. In step 506 it is checked, if a request for the first mobile entity table is received. If it is, the first mobile entity table is sent in step 502 to a predefined set of other firewalls.

This section of SYVANNE et al. discloses sending a first mobile entity table to a predefined set of other firewalls if a predetermined time has elapsed, if a change in the first mobile entity has occurred, or if a request for the first mobile entity table has been received. As noted above, SYVANNE et al. discloses sharing information between firewalls that connect subnetworks to a public network (Fig. 2A, paragraph 0032). SYVANNE et al. further discloses that the firewall system that connects a subnetwork to a private network does not have information about the connections inside the subnetwork (paragraph 0032). Therefore, SYVANNE et al. cannot disclose or suggest a Gi firewall that includes a Gi communication module that is operable to receive an instruction from a GTP communication module of a GTP firewall to tear down a firewall session, a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module, as recited in claim 22.

Paragraph 0010 of KAVANAGH has been reproduced above. This section of KAVANAGH discloses the GTP control messages used to tear down a GTP Tunnel. This section of KAVANAGH does not disclose or suggest a Gi communication module that is operable to receive an instruction from the GTP communication module to tear down a firewall session or a firewall session list. Therefore, this section of KAVANAGH cannot disclose or suggest a Gi firewall that includes a Gi communication module that is operable to receive an instruction from a GTP communication module of a GTP firewall to tear down a firewall session,

a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module, as recited in claim 22. In fact, as noted above, KAVANAGH merely discloses that, in existing GPRS networks, the GTP-Control Plane tears down the tunnel when transmission is finished (paragraph 0007).

In paragraph 0046, KAVANAGH discloses that, since no stateful inspection exists to determine whether a particular message type is permitted, all GTP message types are passed through firewalls. This section of KAVANAGH does not disclose or remotely suggest a Gi firewall that includes a Gi communication module that is operable to receive an instruction from a GTP communication module of a GTP firewall to tear down a firewall session, a firewall session list, and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module, as recited in claim 22.

For at least the foregoing reason, Applicants submit that claim 22 is patentable over SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination.

Claims 23-25 depend from claim 22. Therefore, these claims are patentable over SYVANNE et al. and KAVANAGH, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 22.

Claims 26 and 27 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over SYLVANNE et al. in view of KAVANAGH and GOPAL et al. Applicants respectfully traverse this rejection.

Claims 26 and 27 depend from claim 22. Without acquiescing in the rejection of claims 26 and 27, Applicants submit that the disclosure of GOPAL et al. does not remedy the deficiencies in the disclosures of SYLVANNE et al. and KAVANAGH set forth above with

respect to claim 22. Therefore, claims 26 and 27 are patentable over SYVANNE et al., KAVANAGH, and GOPAL et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 22.

In view of the foregoing remarks, Applicant respectfully requests the Examiner's reconsideration of this application, and the timely allowance of the pending claims.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Meagan S. Walling, Reg. No. 60,112/
Meagan S. Walling
Reg. No. 60,112

Date: June 18, 2008

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808